THE UNIVERSITY OF TEXAS AT SAN ANTONIO, COLLEGE OF BUSINESS

Working Paper SERIES

February 20, 2008

Wp# 0040IS-299-2008

Investigating the impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms

Myung Ko* [a,1], Kweku-Muata Osei-Bryson[b], and Carlos Dorantes[a,2]
[a]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, U.S.A.
Email: [1]myung.ko@utsa.edu, [2]carlos.dorantes@utsa.edu

[b]Department of Information Systems and
The Information Systems Research Institute
Virginia Commonwealth University
Richmond, VA 23284, U.S.A.
Email: Kweku.Muata@isy.vcu.edu

Department of Information Systems and Technology Management,
University of Texas at San Antonio,
San Antonio, TX 78249, U.S.A

Keywords: Information security, impact, security breach, organizational performance, confidentiality, integrity, availability

Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms

Myung Ko* [a,1], Kweku-Muata Osei-Bryson[b], and Carlos Dorantes[a,2]

[a]Department of Information Systems and Technology Management
College of Business
The University of Texas at San Antonio
One UTSA Circle
San Antonio, TX 78249, U.S.A.
Email: [1]myung.ko@utsa.edu, [2]carlos.dorantes@utsa.edu

[b]Department of Information Systems and
The Information Systems Research Institute
Virginia Commonwealth University
Richmond, VA 23284, U.S.A.
Email: Kweku.Muata@isy.vcu.edu

Investigating the Impact of Publicly Announced Information Security Breaches on Three Performance Indicators of the Breached Firms

ABSTRACT:

This paper examines the impact of information security breaches on organizational performance. Up to date, there have been only a few empirical academic studies that have investigated this issue and they have investigated information security breaches with the focus on the short-term impact on the market value of the firm. This study offers an alternate approach to investigate this issue as it explores the impact of breaches on financial performance of the firm, one year after the breach. Using a "matched sampling" methodology**,** we explored the impact of each type of breach (i.e. *confidentiality, integrity*, and *availability*) and also by IT intensity and size. Our results suggest that the direction of the impact (i.e. positive, negative) is dependent on the type of security breaches and also the impact of IT intensive firms is different from non-IT intensive firms. Our study also includes some important implications for managers and stock market investors.

KEYWORDS: Information security, impact, security breach, organizational performance, confidentiality, integrity, availability

JEL Code: M150

INTRODUCTION

Today, as more organizations conduct their businesses over the Internet, exposure to information security attacks is also increasing. The 2004 Global Security Survey of financial institutions by Deloitte and Touche reported that 83 percent of respondents indicated that their systems had been compromised in 2004, compared to 39 percent in the previous year, an increase of over 100% in a single year (Anonymous, 2004). The 2004 E-crime Watch survey by Chief Security Officer (CSO) magazine also reported that 43 percent of respondents noted an increase in information security breaches compared to the previous year and 70 percent had experienced at least one breach incident [1]. Information security breaches include virus, spyware, unauthorized access to information, theft of proprietary information, denial of service (DOS), system penetration, sabotage, and Website defacement, etc. According to the 2005 Computer Crime and Security Survey by CSI-FBI, the average loss per incident from *unauthorized access to information* has increased to $300K from $51K and the loss from *theft of proprietary information* has increased to $356K from $169K, indicating a doubling of such losses compared to 2004 (Gordon et al., 2005; Gordon et al., 2004).

Ponemon Institute reported that total costs for each data breach ranged from less than $1 million to more than $22 million in their 2006 annual study, which investigated financial impact of data breaches involving customers' personal information (Ponemon, 2006). In general, costs of a security breach on organization can classify into short-term and long-term costs (Erbschloe, 2005; Cavusoglu et al., 2004; D'Amico, 2000). For example, short-term costs are costs incurred to deal with the breach immediately after or during the period following the breach and thus, they are short-term in nature. These costs include costs to repair or replace the systems, loss of business or decreased productivity due to the disruption of business operations, and any costs related to reporting information to the public, customers, and business partners about the breach, etc. Long-term costs are costs that can have a significant impact on the organization's future cash flow and thus they have the long-term economic impact and costs incur over several periods. These costs include revenue lost due to the loss of existing or future customers, a decline in investors' confidence due to a negative reputation of the organization, potential legal liabilities from the breach, and reduced goodwill (Cavusoglu et al., 2004; Tsiakis & Stephanides, 2005; D'Amico, 2000; Featherman et al., 2006; Ponemon, 2006). Thus, consequences of a

security breach incident could result in tremendous financial losses to the targeted organization (Warren & Hutchinson, 2000; Egan & Mather, 2005; Garg et al., 2003b).

While there are many news and surveys that have reported the magnitude of the monetary losses from the breach incidents, there have been only a few empirical academic studies that have investigated this issue and these previous studies employed an event study methodology with the focus on an impact on the market value of the firm (Garg et al., 2003a, 2003b; Hovav & D'Arcy, 2003 & 2004; Campbell et al., 2003; Cavusoglu et al., 2004). The event study investigates the stock market reaction to the public announcement of a security breach since there is a belief that this unexpected event can have immediate adverse effect on the breached organization's stock price. Accordingly, such unexpected announcement may lower the market value of the breached organization and thus, the organization can incur a loss or experience a negative abnormal return because the actual return of the stock would be lower than the expected return due to the changes in investors' expectations about the company since the organization can suffer from the public relations exposures than the breach itself. However, it is unclear if this loss will affect the organization's ability to generate revenue in the long term.

Our research objective is to assess the relative magnitudes of the impact on organizational performance of different types of security breaches. In this study, we use the three properties of information security - *confidentiality*, *integrity,* and *availability* - to classify the type of security breach. Thus, this study offers an alternate approach to investigate the impact of publicly announced information security breaches on firms.

Previous event studies examined the market value of the breached firm a few days following the announcement of information security breaches and found the significant negative market reaction. If investors' expectations on the breached firms' future cash flows were true, financial performance of the breached firms would be decreased over time. Although organizational performance is a multifaceted aspect that is difficult to measure, the common proxy is profitability measure (Snow and Hrebiniak, 1980). Thus, this study uses financial performance indicators (e.g., sales and cost of good sold) as surrogates of overall organizational (or financial) performance of the breached organization. To control for profitability of the industry in which the breached firm competes, we calculated the industry benchmark and used it to calculate the "expected" performance of the breached firm, which represents the predicted performance of the

breached firm in absence of the security breach. When this is compared with the financial performance after the breach (refer to as "actual performance"), the difference should represents the effect (abnormal performance) from the security breach.

This research is one of the few academic studies that investigate the impact of the security breach on organizations using financial performance measures, not on the market value of the organizations. Therefore, this study extends the body of knowledge on this research topic. Our study is also important to managers since it helps managers to understand the economic consequences of each type of security breach. It is especially important to managers of IT intensive firms since it appears that these firms have the most security breach events and the negative impact of the breach events is greater than that of non-IT intensive firms.

The paper is organized as follows. In the following section, we review the previous information security breach studies. We then describe the financial performance measures used in this study. The next section describes the previous information security studies, followed by research hypotheses. In the subsequent section, we discuss our research methodology including the sample selection technique and statistical analysis. The results of our analyses are reported and discussed after that. Finally, we conclude with a discussion including implications of our study and suggestions for future research.

OVERVIEW OF PREVIOUS RESEARCH

Several recent studies have investigated the impact of public announcements of various security breaches on the market value of a firm using an event study methodology. These studies are based on the assumption that capital markets are efficient to evaluate the impact of the events on expected future profits of the firms (Dasgupta, et al., 1998). However, results from these studies on security breach announcements are somewhat mixed. Some studies found a significant negative market reaction after a security breach is publicly announced. Cavusoglu et al. (2004) found that announcement of security breach is negatively associated with the market value of the breached firm. Their study indicated that the breached firms lost on average 2.1 percent of their market value within two days of the announcement and the loss was larger for Internet firms than for conventional firms. Their study also indicated that Internet security developers realized significant positive return from the announcement. Garg et al. (2003b) also

reported that all types of security breaches realized a negative abnormal return over a three-day period from the announcement. However, their study reported that security breaches related to credit card information theft realized the most significant negative impact. In addition, the market value of security companies realized a positive impact to security breaches. Acquisto et al. (2006) investigated privacy breaches and found that a significant negative impact on a firm's market value on the day of breach announcement. However, this effect decreased over the day following the breach announcement.

On the other hand, some studies found either no significant impact or significant impact on only certain types of security breaches. Hovav & D'Arcy (2004) investigated the market reaction to virus attack announcements and found that there is no significant impact over the 0 to 25 days from the announcement. Hovav & D'Arcy (2003) investigated the market reaction to denial-of-service (DOS) attack announcements for a period from 0 to 25 days and found negative average abnormal returns on average 48.6 percent of the breached companies. These negative abnormal returns were greater for Internet-specific companies than those of the non-Internet-specific companies.

Campbell et al. (2003) examined the stock market reaction to security breaches for a period of 0 to 3 days from the announcement and found that not all types of security breaches have similar economic impact. The authors found that a significant negative reaction for those breaches that are related to confidential information and did not find any significance from the other types of breaches.

Focusing only on one type of security breaches, such as "unauthorized access to confidential data," Ko and Dorantes (2006) investigated the impact on financial performance of the breached firm for each of four quarters after the incident. The authors selected a control firm that is comparable to the breached firm, based on size and industry and then compared the performance of each sample. The authors found that the performance of the control sample was higher compared to that of the breached firms in general. Table 1 includes a brief summary of the previous information security breach studies.

Table 1: Summary of previous security breach studies

Author	Period studied	Sample size	Research methodology	Focus of study	Major findings
Campbell et al. (2003)	1995 – 2000	43	Event study	Two types (access to confidential or not)	• a significant negative return involving confidential information and no changes in return for other types of breach
Garg et al. (2003b)	1996 – 2002	22	Event study	All	• on average, the loss is 2.7 percent over one day and 4.5 percent over a three-day period.
Hovav & D'Arcy (2003)	1998 – 2002	23	Event study	DOS attacks	• significant negative abnormal returns on a half of the breached companies • the negative abnormal returns of the Internet-specific companies were larger
Hovav & D'Arcy (2004)	1988 – 2002	186	Event study	Virus attacks	• no negative returns over 5 days after the announcement • a half of the sample experienced negative returns 25 days after the announcement
Cavusoglu et al. (2004)	1996 – 2001	66	Event study	All types	• a negative return on the market value of the breached firm and a positive return of the Internet security developer
Acquisto et al. (2006)	2000 – 2006 (3/01)	79	Event study	Privacy (misuse of personal data)	• a moderate but significant negative impact on a firm's market value
Ko & Dorantes (2006)	2000 – 2003	19 Matched sample (treatment vs. control) comparison		Confidential data	• the control firms outperformed the breached (treatment) firms in general

In general, majority of the previous studies that have investigated the impact of publicly announced information security breach incidents found a significant negative impact. However, depends on the types of security breaches, some found no significant impact. Further these

studies have focused their attention on the on the market value of the firm rather than on the financial performance of the firm.

FINANCIAL PERFORMANCE INDICATORS

Financial ratios are the most commonly used performance indicators in evaluating the performance of a firm and their usefulness has been demonstrated in many empirical studies (Barney, 1997; Chen and Shimerda, 1981; Hitt & Brynjolfsson 1996; Bharadwaj 2000; Hunton et al. 2003; Nicolaou 2004). In this study, we used two profit ratios (ROA and ROS) and one cost ratio (COGS/S). Return on assets (ROA) is the most frequently used as a performance indicators and a useful indicator to measure how profitable a company is (Bharadwaj, 2000; Hunton et al., 2003; Grover & Saeed, 2004). Return on sales (ROS) is another indicator that measures firm's profitability. Thus, the higher the profitability ratio is, the more profitable the organization is. Cost of goods sold to sales (COGS/S) measures the percentage of sales used to pay for expenses related to sales. Thus, the higher the cost ratio is, the less profitable the organization is since it represents the increase in costs. It should be noted that stock markets also use these financial performance indicators to predict the price of a firm's stock. Table 2 presents the descriptions of the financial performance measures.

Table 2: Description of Financial Performance Measures

Performance Variable	Description
Return on Assets (**ROA**)	Operating Income before Depreciation / Total Assets
Return on Sales (**ROS**)	Operating Income before Depreciation / Net Sales
Cost of Goods Sold to Sales (**COGS/S**)	Cost of Goods Sold / Net Sales

While these performance indicators are useful in understanding firm's financial condition, they should be used with caution. When the breached firm's performance indicators are compared with those of a non-breached firm without controlling for industry profitability, these performance indicators are confounded due to the effects of intra-industry and inter-industry variation (Dess and Robinson, Jr., 1984).

In this study, we matched the breached firm with control firms that are operated in the same industry to compare the difference in performance. Therefore, there is no effect on inter-industry

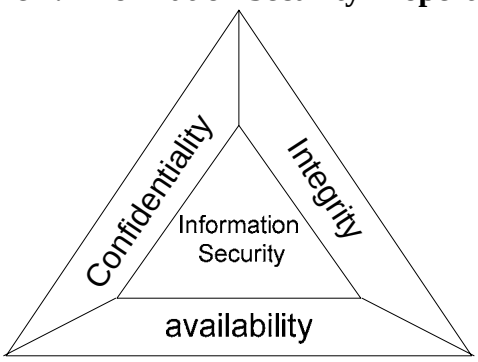
variation but the effect of intra-industry variation still needs to be controlled. Accordingly, the profitability of the industry within which the breached firm competed during the period for our test was identified as an industry benchmark and used it to account for the effects of intra-industry variation. See Statistical Analysis section for the detailed information.

INFORMATION SECURITY

Information security includes three properties – *Confidentiality*, *Integrity*, and *Availability* (Ezingeard et al., 2005; Pfleeger, 1997; Solomon and Chapple, 2005). Each property composes one leg of the triad as shown in Figure 1 and thus it is known as the "CIA Triad."

- *Confidentiality* refers to the protection against unauthorized access to data and system information and it ensures that only authorized parties can view the data and execute processes.
- *Integrity* refers to the prevention of accidental or malicious alteration, corruption, or deletion of data or information or systems. It ensures that only authorized parties can modify it in authorized manners.
- *Availability* refers to the prevention and recovery from hardware and software errors and from malicious data denials. It ensures that authorized parties have access to information when needed.

Figure 1: Information Security Properties (CIA Triad)

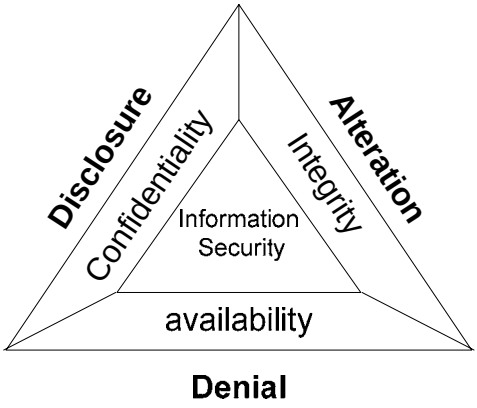


(Source: Solomon and Chapple, 2005)

There are three primary mechanisms that are used by malicious individual to defeat these three information security properties and they are the disclosure, alteration, and denial, and the

model is known as the "DAD Triad" (Solomon and Chapple, 2005). Each of these DAD Triad components closely relates to the CIA Triad components as shown in Figure 2.

Figure 2: DAD Triad



(Source: Solomon and Chapple, 2005)

Disclosure can happen when organizations fail to ensure confidentiality property of information security in the CIA Triad. Accordingly, we assume that *confidentiality* of information security is related to security breaches involving *unauthorized access to confidential information* incidents. *Alteration* can happen when organizations fail to ensure integrity of information security and thus *integrity* relates to security breaches such as *website defacement* and *corruption of information* due to viruses or worms incidents. *Denial* can happen when organizations fail to ensure availability of information security and thus, *availability* relates to security breaches such as *denial of services* incidents. Based on the discussion of the CIA Triad and the DAD Triad, we classified security breach incidents into breaches of *confidentiality*, *integrity*, and *availability* in our study.

RESEARCH MODEL AND HYPOTHESES

The previous research (i.e., Campbell et al., 2003; Garg et al., 2003b; Acquisto et al., 2006) identified that information security breaches involving *Confidentiality* breaches (i.e. *unauthorized access to confidential information*) have a statistically significant negative market returns on firms. Thus, the following hypotheses were proposed.

H1A: The *Return on Assets (ROA)* of a firm that has experienced an information security breach involving *Confidentiality* is lower following year subsequent to breach than the year before the breach, compare to the firms that are similar in size and operate in the same industry as the breached firm.

H1B: The *Return on Sales (ROS)* of a firm that has experienced an information security breach involving *Confidentiality* is lower following year subsequent to breach than the year before the breach, compare to the firms that have the similar in size and operate in the same industry as the breached firm.

H1C: The *Cost of Goods Sold to Sales (COGS/S)* of a firm that has experienced an information security breach involving *Confidentiality* is higher following year subsequent to breach than the year before the breach, compare to the firms that are similar in size and operate in the same industry as the breached firm.

On the other hand, the previous research (i.e., Campbell et al., 2003; Hovav & D'Arcy, 2004) indicated that information security breaches involving *Integrity* breaches (i.e., *Corruption of Information due to virus* or *worms*, *Website Defacement*) have no statistically significant impact on market returns on firms and we would expect no changes in financial performance of the breached firm. Thus, the following hypotheses were proposed.

H2A: Compare to the firms that are similar in size and operate in the same industry as the breached firm, there is no significant change in the *Return on Assets* (ROA) of a breached firm following year subsequent to breach than the year before the breach when it relates to *Integrity*.

H2B: Compare to the firms that are similar in size and operate in the same industry as the breached firm, there is no significant change in the *Return on Sales* (ROS) of a breached firm following year subsequent to breach than the year before the breach when it relates to *Integrity*.

H2C: Compare to the firms that are similar in size and operate in the same industry as the breached firm, there is no significant change in the *Cost of Goods Sold to Sales* (COGS/S) of a breached firm following year subsequent to breach than the year before the breach when it relates to *Integrity*.

Sim ilar to *Confidentiality* breaches, the previous research (i.e., Hovav & D'Arcy, 2003) also indicated that information security breaches involving *Availability* breaches (i.e., *Denial of Service*) have a statistically significant negative market returns on firms. Thus, the following hypotheses were proposed.

H3A: The *Return on Assets* (ROA) of a firm that has experienced an information security breach involving *Availability* is lower following year subsequent to breach than the year before the breach, compared to the firms that are similar in size and operate in the same industry as the breached firm.

H3B: The *Return on Sales* (ROS) of a firm that has experienced an information security breach involving *Availability* is lower following year subsequent to breach than the year before the breach, compared to the firms that are similar in size and operate in the same industry as the breached firm.

H3C: The *Cost of Goods Sold to Sales* (COGS/S) of a firm that has experienced an information security breach involving *Availability* is higher following year subsequent to breach than the year before the breach, compared to the firms that are similar in size and operate in the same industry.

Given the expectation that information security breaches can be associated with various short term and long term costs, such as costs of repairs, legal liability, and negative reputation, we would expect that a breached firm's profit ratios will be decreased and its cost ratio will be increased after a security breach. Thus, the following hypotheses regarding the overall impact on the breached firm were proposed.

H4A: The *Return on Assets (ROA)* of a firm that has experienced an information security breach is lower following year subsequent to breach than the year before the breach, compare to the firms that are similar in size and operate in the same industry as the breached firm.

H4B: The *Return on Sales (ROS)* of a firm that has experienced an information security breach is lower following year subsequent to breach than the year before the breach, compare to the firms that are similar in size and operate in the same industry as the breached firm

H4C: The *Cost of Goods Sold to Sales (COGS/S)* of a firm that has experienced an information security breach is higher following year subsequent to breach than the year before the

breach, compare to the firms that aresimilar in size and operate in the same industry as the breached firm.

RESEARCH METHODOLOGY

This study employs a "matched sampling" methodology to construct control firms. This methodology has also been used in several previous studies (e.g., Balakrishnan et al., 1996; Hunton et al., 2003; Bharadwaj, 2000; Barber and Lyon, 1996) and appeared to be most appropriate to test our hypotheses for following reasons. First, financial performance of the control firms that are matched by industry and size of the breached firms can be used as an industry benchmark. Second, it helps control for any confounding factors coming from diverse industries and size.

While the previous studies that used the "matched sample" methodology comparing each treatment firm with only one control firm (e.g., Bharadwaj, 2000), this study includes multiple control firms that met matching criteria for each treatment firm. More detailed information about selection of control firms is documented in the Sample Selection for 'a Control Sample.'

Sample Selection

A Treatment Sample (Breached Firms)

Our sample includes publicly announced all information security breach incidents for the period from 1997 to 2004 but including announcements of publicly traded firms. Following procedures are taken to select our sample.

We collected data using business news articles in the Lexis/Nexis Academic database. The key words used to search the data are "attack," "breach," "break-in," "hacker," "Internet," "security," "virus," "information," and "computer." A combination of such key words, names of breached firms that were reported in previous studies, and names of viruses that were identified in previous studies were also used. This approach is similar to the method used by previous studies (Cavusoglu et al., 2004; Campbell et al., 2003; Andoh-Baidoo & Osei-Bryson, 2006). Initially, the data set included 105 cases. First, all duplicated announcements were eliminated. Then, announcements related to non-public firms were eliminated. After eliminating cases with missing financial data from *Compustat* and eliminating two outliers from the sample, the final

treatment sample was reduced to 69. Then the treatment sample was classified into *Confidentiality*, *Integrity*, and *Availability* incidents. Table 3 includes the descriptive statistics of the breached firms (treatment sample), Table 4 provides the distribution of the information security breaches by year, Table 5 provides the distribution of the breaches by type, and Table 6 provides the distribution of the treatment sample by industry. It indicates that business services industry (i.e., SIC code: 73) incurred the most of the information security breach events.

Table 3: Descriptive Statistics of the Sample

Variable	Mean	Min	Max	Std. dev.
Total assets ($Million)	74,685	13	1,484,101	206,406
Sales ($Million)	17,041	1	170,064	26,219

Table 4: Distribution of Information Security Breaches by Year

Year	Number of incidents
1997	2
1998	3
1999	12
2000	24
2001	6
2002	5
2003	11
2004	6
Total	69

Table 5: Distribution of Information Security Breaches

Property	Type of Security Breaches	Number of incidents
Confidentiality	Unauthorized access to confidential information	18
Integrity	Website Defacement & Corruption of information due to virus or worm	31
Availability	Denial of Service	20
Total		**69**

Table 6: Distribution of the Breached Firms by Industry

Two Digit SIC Code	Industry Description	Number of Firms
27	Printing and publishing	4
28	Chemical and allied products	2
30	Rubber and misc. plastics products	1
35	Industrial machinery and equipment	5
36	Electronic & other electronic equipment	1

Two Digit SIC Code	Industry Description	Number of Firms
37	Transportation equipment	3
45	Air transportation	2
48	Communication	8
49	Electric, gas, & sanitary services	1
59	Misc. retail	4
60	Depository Institutions	5
61	Non-depository institutions	3
62	Security & commodity brokers	4
73	Business services	25
78	Motion pictures	1
Total		**69**

A Control Sample (Industry Benchmark)

To select control firms, which are comparable to size and industry of the treatment sample, firms that operated in the breached firm's two digit industry code are selected. For the firm size, we used total asset, which is a commonly used proxy for firm size (Hunton et al., 2003).

We followed two major steps in selecting control firms. Firstly, we selected all firms with the same two-digit SIC code (industry) as the breached firm from the Compustat database. To control for the firm size from the pre-selected firms from selected firms whose total assets was between 70% and 130% of the breached firm's total assets in the year of security breach incident Thus, one or more matching control firms were selected for each breached firm. As a result, the average number of control firms per each breached firm was 42^2. It should be noted that this is an established and frequently used approach in finance and accounting (Barber & Lyon 1996).

STATISTICAL ANALYSIS

Abnormal Performance

Abnormal performance represents the difference between the actual and expected performance of the breached firm. The actual performance represents the breached firm's financial performance at one year after the breach, which measured in terms of performance indicators (e.g., ROA, ROS and COGS/S). The expected performance represents the predicted financial performance of the breached firm at one year after the breach in absence of the security breach event. Thus, if the actual and expected performance is same, then, the difference in

performance is zero (0), if the actual performance is greater than the expected performance, the difference in performance is greater than zero (0), otherwise, it is less than zero (0).

To calculate the expected performance, start with financial performance of the breached firm a year before the breach and add the overall change in industry profitability during the period from a year before the breach and a year after the breach. This change is called an industry benchmark (see the calculation below) and it is used to control for any effect from the intra-industry variation during the period.

Following Barber and Lyon (1996)'s method, calculation of the expected performance of the breached firms is done in two steps as follows. First, calculate the overall pre-incident industry performance from each control sample that may include one or more matching firms by size in the same industry for each breached firm ($PControl_{t-1}$). This is repeated for the year subsequent to the breach (*year t+1)* to calculate post-incident performance of the control sub-sample $(PControl_{t+1})$. Then, difference between industry's pre-incident *(year t-1)* performance and post-incident *(year t+1)* performance represents the *industry benchmark*, Δ *PIndustry,* shown as below.

$$\Delta\ PIndustry = PControl_{t+1} - PControl_{t-1} \quad (1)$$

where *t* is a year of the security breach.

Second, the expected post-incident performance of the breached firm, $Expected(PTreat_{t+1})$, in the absence of an incident is calculated by adding any changes in the industry's performance, $\Delta PIndustry$, to the breached firm's pre-incident performance, $PTreat_{t-1}$, as follows:

$$Expected(PTreat_{t+1}) = PTreat_{t-1} + \Delta\ PIndustry \quad (2)$$

Finally, the difference in abnormal performance of the breached firm, $Abnormal(PTreat_{t+1})$, is calculated as the actual post-incident performance, $Actual(PTreat_{t+1})$, minus the expected post-incident performance, $Expected(PTreat_{t+1})$ as follows:

$$Abnormal(PTreat) = Actual(PTreat_{t+1}) - Exp(PTreat_{t+1}) \quad (3)$$

For the ROA & ROS measures, Abnormal $(PTreat) > 0$ if the actual performance is higher than the expected performance ($Actual(PTreat_{t+1}) > Expected(PTreat_{t+1})$) and Abnormal$(PTreat) < 0$ if otherwise; for the COG/S measure, Abnormal $(PTreat) < 0$ if the actual performance is higher

than the expected performance ((*Actual(PTreat$_{t+1}$) < Expected(PTreat$_{t+1}$)*) and Abnormal*(PTreat)> 0* if otherwise.

To test whether the mean difference of the abnormal performance of the treatment firms comparing to the control firms, we used one-tailed one-sample t-test. We also determine if it reaches the threshold of statistical significance.

RESULTS AND DISCUSSION OF FINDINGS

We ran one-sample t-test for each category of security breaches to determine if the breached firm's actual performance is less than the expected performance a year after the breach to test H1A to H3C. Then, we also ran the t-test for all data to determine the overall effect on the breached firms' performance to test H4A to H4C. The results from each category of breach are reported as the following:

The Impact of Confidentiality Breaches

Table 7 displays the results of our analysis of the long-term impacts of *Confidentiality* breaches. While there is some evidence that the impact of *Confidentiality* breaches on organizational performance is mixed since there was a negative long-term impact on ROA and COGS and positive long-term impact on ROS, these results are not statistically significant at even the 10% significance level. Thus, we concluded that all three hypotheses, H1A, H1B, and H1C are not supported.

Table 7: Abnormal Performance – *Confidentiality Breaches*

Performance Measure	Sample Size	Mean	t-test	p value (1-tailed)
Abnormal performance of ROA	18	-0.017 ↓	-0.554	0.293
Abnormal performance of ROS	18	0.009 ↑	0.265	0.397
Abnormal performance of COGS/S	18	0.089 ↓	1.285	0.108

Since Confidentiality breaches involve unauthorized access to data or system information, it may seem reasonable to expect that the occurrence of this type of breach can lead to long-term damage to a firm's reputation including loss of trust by customers which can result in the firm loosing customers to its competitors. On the other hand a breach involving a virus attack that is not directed specifically at the given firm is unlikely to result in long-term damage to the firm's

reputation. We conducted statistical analysis to explore differences in the impacts of *Confidentiality* breaches and Virus attacks, with the result being that there was no statistically significant difference between impacts of these two different types of breaches.

The Impact of Integrity Breaches

Table 8 displays the results of our analysis of the long-term impacts of *Integrity* breaches. While there is some evidence that the impact of *Integrity* breaches on organizational performance is mixed since there was a negative long-term impact on ROA and positive long-term impact on ROS and COGS, these results are not statistically significant at even the 10% significance level. Since the financial performance of the breached firms did not change significantly, we concluded that all three hypotheses, H2A, H2B, and H2C are supported.

Table 8: Abnormal Performance – *Integrity Breaches*

Performance Measure	Sample Size	Mean	t-test	P value (1-tailed)
Abnormal performance of ROA	31	-0.057 ↓	-1.184	0.123
Abnormal performance of ROS	31	0.137 ↑	0.837	0.205
Abnormal performance of COGS/S	31	-0.008 ↑	-0.173	0.431

The *Integrity* breaches that occurred in the firms of our sample involve two subtypes: *Website Defacement* or *Corruption of Information due to virus or worm*. Since *Corruption of Information due to virus or worm* involve technical damage which often be easily repaired in a relatively short-time with but no other damages, it seems reasonable to assume that it might have a minimal long-term impact on a firm's performance. However the estimated cost of well known virus, ILOVEYOU, ranged between less than $1 billion to $15.3 billion in software damage and computer downtime (Grabosky, 2007) and it reached approximately 45 million users in one day (SearchSecurity.Com, 2006). On the other hand, *Website Defacement* may have detrimental impact on the credibility and reputation of the organization, leading to long-term damage including loss of customer trust and loss of revenue (Hollander , 2000). We conducted statistical analysis to explore differences in the impacts of *Corruption of Information* and *Website Defacement* breaches, with the result being that there was no statistically significant difference between impacts of these two different subtypes of *Integrity* breaches.

The Impact of Availability Breaches

Table 9 displays the results of our analysis of the long-term impacts of *Availability* breaches. While there is some evidence that the impact of *Availability* breaches on organizational performance is mixed since there was a negative long-term impact on ROA and ROS and positive long-term impact on COG/S, only the result involving ROA is statistically significant at the 10% significance level. Thus, we concluded that H3A is supported and H3B and H3C are not supported.

Table 9: Abnormal Performance – *Availability Breaches*

Performance Measure	Sample Size	Mean	t-test	p value (1-tailed)
Abnormal performance of ROA	20	-0.090 ↓	-1.515	0.073 [a]
Abnormal performance of ROS	20	-0.044 ↓	-0.688	0.250
Abnormal performance of COGS/S	20	-0.046 ↑	-0.593	0.280

[a] 10 % level

Estimated cost of *Denial of Service* incidents was over $65 million in 2003 CSI/FBI Computer Crime and Security Survey, which was the second most expensive breached incident (Williams and Joshi, 2004). Since *Denial of Service* (DOS) attack is targeted at the breached firms, its intention is to destroy a business, its reputation, and its resources, it reasonable to expect that this type of breach may have a greater long term impact on organizational performance than Virus attacks, since the latter is not targeted at the specific firm but affects many firms, these firms make effort to repair such damage quickly as possible as the entire market as a whole. We conducted statistical analysis to explore differences in the impacts of *Denial of Service* and *Virus Attack* breaches, with the result being that there was no statistically significant difference between impacts of these two different types of breaches.

The Impact of Overall Security Breaches

Table 10 displays the results of our analysis of the overall long-term impacts. While there is some evidence that the long-term impact of security breaches on organizational performance is a negative long-term impact, ROA is the only measure with statistically significant long-term

negative impact at even the 10% significance level. Thus, we concluded that hypotheses, H4A is supported but H4B and H4C are not supported.

Table 10: Abnormal Performance - Overall

Performance Measure	Sample Size	Mean	t-test	p value (1-tailed)
Abnormal performance of ROA	69	-0.056 ↓	-1.966	0.027[b]
Abnormal performance of ROS	69	0.051 ↓	0.671	0.253
Abnormal performance of COGS/S	69	0.006 ↓	0.177	0.430

[b] 5 % level

To better understand if impact of security breaches of the firms has different consequences depending on its IT intensity, we followed Chatterjee's (2001) classification of industries according to IT roles into the categories of *Automate*, *Informate-Up-and-Down*, and *Transformative*. *Automate* firms usually replace expensive human labor with IT; *Informate-Up-and-Down* firms usually provide information to empower employees and give more control to management; *Transformative* firms radically change traditional ways of doing business by redesigning business processes, structures and relationships and the bank is an example of transformative industry. Within this classification scheme the *Transformative* category is considered to be more IT intensive than the *Automate* or *Informate-Up-and-Down* categories.

Table 11: Overall Cases by Breach Type and IT Intensity Category

IT Intensity Category/ Breach Type	Confidentiality Breaches	Integrity Breaches	Availability Breaches	Total Number of incidents
Automate 0		5	2	7
Informate-up-and-down 3		7	1	11
Transformative 15		19	17	51
Total	18 31		20	69

Table 11 shows the breakdown by types of breach and IT intensity category. Interestingly, over 70% of security breach events in our sample are from firms in the *Transformative* category. Given this breakdown and our interest in exploring the effect of IT intensity on the impact of security breaches, we conducted analysis on the impact of the security breaches for the *Transformative* IT intensity category (see Table 12) and the other two less-IT intensive categories (see Table 13). Both the ROA and COGS/S measures were statistically significant for

the *Transformative* IT intensity category, the results suggesting that security breaches have a long-term impact on the performance.

Table 12: Abnormal Performance - *Transformative Industry*

Performance Measure	Sample Size	Mean	t-test	P value (1-tailed)
Abnormal performance of ROA	51	-0.086 ↓	-2.456	0.009[a]
Abnormal performance of ROS	51	-0.038 ↓	-1.105	0.137
Abnormal performance of COGS/S	51	0.535 ↓	1.942	0.029[a]

[a] 5 % level

Table 13: Abnormal Performance – *Automate* and *Informative-Up-and-Down*

Performance Measure	Sample Size	Mean	t-test	P value (1-tailed)
Abnormal performance of ROA	18	0.026 ↑	0.622	0.271
Abnormal performance of ROS	18	0.303 ↑	1.110	0.142
Abnormal performance of COGS/S	18	-0.127 ↑	-1.153	0.133

We also explored the difference in the mean impacts for *Transformative* IT intensity category and the other two less-IT intensive categories (see Table 14a). These results suggest that with regards to the ROA & ROS measure, that the negative impact on the *Transformative* IT intensity category is more severe than for the other two less-IT intensive categories for the three types of security breaches.

Table 14a: Difference in Abnormal Performance by Breach Type and IT Intensity

Breach Type	IT Intensity	Mean Abnormal ROA	Mean Abnormal ROS	Mean Abnormal COGS/S
Confidentiality	*Non-Transformative*	0.105	0.073	0.332
	Transformative	-0.423	-0.004	0.042

Breach Type	IT Intensity	Mean Abnormal ROA	Mean Abnormal ROS	Mean Abnormal COGS/S
Integrity	*Non-Transformative*	0.002	0.432	-0.126
	Transformative	-0.093	-0.049	0.066
Availability	*Non-Transformative*	0.051	0.016	-0.591
	Transformative	-0.115	-0.054	0.050

We also did a comparison of pairs of breach types and IT intensity categories (see Table 14b). It may be noted that with regards to the ROA measure that the long term damage to *Transformative* firms is more severe than the corresponding damage to *non-Transformative* firms. With regards to the COGS/S measures, the long-term damage to *non-Transformative* firms is far less severe than the corresponding damage to *Transformative* firms.

Table 14b: Abnormal Performance –*Comparison of Breach and IT Intensity*

Comparison	Mean ROA	p value (one-tailed)	Mean ROS	p value (one-tailed)	Mean COGS/S	P value (one-tailed)
Non-Transformative & Confidentiality	0.105	0.06	0.073	0.241	0.332	0.262
Transformative and Availability	-.115		-0.545		0.050	
Non-Transformative & Integrity	0.002	0.43	0.032	1	0.133	-0.125	0.047
Transformative and Availability	-.115		-0.545		0.050	
Non-Transformative & Availability	0.051	0.01	0.385	6	-0.590	0.420	0.075
Transformative &Confidentiality	-0.042		-0.004		0.042	
Non-Transformative & Integrity	0.002	0.43	0.163	1	-0.126	0.156	0.052
Transformative & Confidentiality	-0.042		-0.004		0.042	
Non-Transformative & Confidentiality	0.105	0.07	0.163	3	0.218	0.332	0.273
Transformative & Integrity	-0.093		-0.049		0.066	
Non-Transformative &	0.051		0.016		-0.591	

Comparison	Mean ROA	p value (one-tailed)	Mean ROS	p value (one-tailed)	Mean COGS/S	P value (one-tailed)
Availability						
Transformative & Integrity	-0.093	0.258	-0.049	0.343	0.066	0.071

We then did an analysis by Firm Size by categorizing firms as being Large or Small based on total assets followed approach taken by Hunton et al. (2000). As shown in Table 15, cases are closely distributed by category of breach for both *Large* and *Small* firms.

Table 15: Overall Cases by Breach Type and Firm Size

Firm Size	Confidentiality Breaches	Integrity Breaches	Availability Breaches	Total Number of incidents
Large 9		18	10	37
Small 9		13	10	32
Total	18 31		20	**69**

Table 15a: Difference in Abnormal Performance by Breach Type and Firm Size

Breach Type	Firm Size	Mean ROA	Mean ROS	Mean COGS/S
Confidentiality	*Small*	-0.007	0.029	0.155
	Large	-0.028	-0.012	0.025
Integrity	*Small*	-0.111	0.296	0.036
	Large	-0.017	0.022	-0.040
Availability	*Small*	-0.123	-0.085	0.018
	Large	-0.057	-0.003	-0.110

In general, difference in abnormal performance is less for large firms than small firms except for ROA and ROS of *Confidentiality* as shown in Table 15a. Large firms that have experienced *Confidentiality* breach incidents seem to suffer more and their performance decreased more than the smaller firms in terms of ROA and ROS indicator. This might be due to the difference in media coverage or damage of firm's reputation. Large firms are well recognized by public, compared to smaller firms and thus, these large firms might have had significant effect on sales,

reflected by the perception of their customers, especially on the fact that firms are not handling their confidential information properly.

CONCLUSION AND DISCUSSION OF FINDINGS

Over the past few years, ensuring security of organizational information has been a challenging task for managers due to a continuously increasing security breach incidents (Egan & Mather, 2005; Doherty and Fulford, 2005). While other previous studies have explored the impact of security breaches on the market value of the firm, this study is one of the few academic studies that investigate the impact of the security breach incidents on the organizational performance using financial performance indicators, not on the market value of the organizations.

We identified the actual and expected performance of the firm a year before the breach and captured abnormal performance of the breached firm to investigate the difference in financial performance due to the security breach event. Based on this analysis, the results can be one of three possible situations as following. If abnormal performance of the profitability indicators, such as ROA and ROS shows the negative value, it indicates that performance of the breached firm has decreased after the breach. If it is 0, the performance of the breached firm is the same as before even after the breach. If it is the positive value, the performance of the breached firms has increased after the breach. In the case of the costs indicators, such as cost of goods sold, opposite is true.

In general, the breached firms' abnormal performance of the profitability indicators in our study suggests that except for the *Integrity* breach category, security breaches can have a long-term negative impact on the performance of the breached firm.

Our results suggest that both *Confidentiality* and *Availability* breaches could be considered to each have a long-term negative impact on organizational performance, while Integrity breaches have no long-term negative impact on organization:

- *Confidentiality*: To the extent that *Confidential Information* is a strategic business asset, particularly for firms that are *Large* and/or *Transformative*, it is not surprising that damage to the firm would remain even a year after the incident since a breach could result in loss of

competitive advantage. This suggests that with regards to *Confidentiality* breaches, the security strategy has to be heavily oriented towards knowledge of & monitoring of potential intruders & prevention of breaches since recovery strategies may not eliminate the long-term effects of this breach. For as has been said before, once lost confidentiality cannot be restored.

- *Integrity*: As discussed previously, this type of breach includes *Corruption of Information*, and *Defacement of Websites*. With regards to *Corruption of Information*, the Semantic Integrity subsystem and Backup & Recovery subsystems of many DBMS offer possibilities for effective recovery strategies and the occurrence of *Corruption of Information* requires additional recovery effort as well as the need for improved detection & prevention systems. With the increasing availability on better techniques, methods, and tools for the design & development of effective & efficient user interfaces, breaches involving *Defacement of Websites* could motivate firms to take advantage of such resources resulting in better & more cost effective websites.
- *Availability*: The results appear to suggest that the impact of security breaches could be long-term. Part of the issue here is the importance of the Internet to the given business, including how long could it function without some or all of its internet services. Thus the firm has to have a good understanding of the relationship between its critical business operations and Internet access, as well as knowledge of the business objectives of its competitors and other potential attackers.

So what is the implication of these results, some of which go against our initial expectations?

There are three competing arguments regarding to the impact of information security breaches. First, security breaches can have a long-term negative financial impact on firms. This position appears to be supported by our results for *Availability* and *Confidentiality* breaches but not for *Integrity* breaches. Second, most of security breaches have no impact or minimum impact on firms. This position appears to be supported by our results for *Integrity*. In addition, another argument is that firms make new investments in information security as a result of the breaches and these investments may lead to long-term economic benefits. Thus, a third argument is that security breaches may have a net positive long-term impact on firms (Campbell et al., 2003). This third position appears not to be supported by our results.

While stock market investors tend to unload the breached firm's stock after a breach possibly because they believe that the breached firm has been damaged and it has substantial economic consequences, it appears that for *Integrity*, any such damage was at most temporary and that the breached firms were able to recover and perform even better than before. One possible explanation is that the breached firm may be able to address any weaknesses in information security in a timely manner, which prevented sustained damage. Another possibility is that the breached firm may be investing resources to improve further (Campbell et al., 2003). As a result, the organization became more disciplined, efficient, and effective after the breach.

IMPLICATIONS AND LIMITATIONS

Our results have important implications for top managers and stock market investors. First, protection of confidential information has to be ensured. Well-defined security policies and procedures are a necessary step toward an effective information security program. Also any known vulnerabilities to security must be managed to ensure regaining the confidence of overly concerned investors. Second, although the market value of the breached firm might drop temporarily as indicated in the previous event studies, overall negative impact on the firm's financial performance might be short-term for some types of information incidents (i.e. *Integrity*) or depends on the type of industries in which firms operate (i.e. *Automate* or *Informate-Up-and-Down*). Our study indicated that *Transformative* firms are most impacted by security breaches. Thus, managers in those industries should adequately equipped with defense mechanisms to mitigate any potential source of threat or vulnerability, especially in the case of *Confidentiality* or *Availability* breaches.

Thirdly, given the difficulty of recovering from *Confidentiality* breach incidents, primary emphasis has to be placed on strategies to prevent the occurrence of this type of breach, and secondary emphasis to prevention and recovery with regards to *Availability* breaches. Such strategies would involve technical (e.g. competitor analysis, detection, protection, and recovery), human, organizational, and possibly inter-organizational components. Further, they require the organization to have an operational-level of understanding of the value of its information and knowledge assets both to itself as well as to potential intruders (e.g. competitors, players in financial markets, employees, etc).

Our study is not without limitation. It is possible that the majority of breached firms included in our sample might be large firms since they are publicly known firms and so might not represent the overall breached firms in general. In addition, range of media coverage and extensiveness of customer perception about the breach, other major business announcements such as a merger, adoption of new technology, or change in top management might have had a significant effect on sales and operating income. Thus, such factors that have not accounted in this study might have biased the results. Further research might be needed including more current security breach events and also including longer than a year after the breach to investigate if the breach has a material impact on the long-term financial performance.

ACKNOWLEDGEMENT:

We thank the associate editor and anonymous reviewers for their valuable comments that significantly improved the quality of this paper.

This research was supported in part by a grant from the 2007 Summer Research Program of the School of Business of Virginia Commonwealth University, Richmond, VA, U.S.A. and was also support by the University of Texas at San Antonio, College of Business 2007 Summer Research Grant.

REFERENCES

Acquisto, A., Friedman, A. and Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study, *Twenty-Seventh International Conference on Information Systems*, 1563 - 1580.

Andoh-Baidoo, F. K. & Osei-Bryson, K-M. (2007). Exploring the Characteristics of Internet Security Breaches that Impact the Market Value of Breached Firms, *Expert Systems with Applications*, **32** (3), April, 703 -725.

Anonymous. (2004). Security Attacks on IT Systems More Than Double, According to Respondents of Deloitte & Touche's Global Financial Services Survey. PR Newswire Association Inc, May 27, available at http://www.prnewswire.com.

Balakrishnan, R., Linsmeier, T. J., & Venkatachalam, M. (1996). Financial Benefits from JIT Adoption: Effects of Customer Concentration and Cost Structure, *Accounting Review,* **71** (2), 183-205

Barber, B. M., & Lyon, J. D. (1996). Detecting Abnormal Operating Performance: The Empirical Power and Specification of Test Statistics, *Journal of Financial Economics*, **41**, 359-399.

Barney, J. B. (1997). Chapter 2: What is Performance? In: Gaining and Sustaining Competitive Advantage, Boston, MA: Addison-Wesley, 30-64.

Bharadwaj, A.S. (2000). A Resource-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation, *MIS Quarterly*, **24** (1), 169-196,

Campbell, K., Gordon, L., Loeb, M. & Zhou, L. (2003). The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market, *Journal of Computer Security,* **11**, 431–448.

Cavusoglu, H., Mishra, B. & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers, *International Journal of Electronic Commerce*, Fall, **9** (1), 69-104.

Chatterjee, D., Richardson, V.J., and Zmud, R.W. (2001). Examining the shareholder wealth effects of announcements of newly created CIO positions, *MIS Quarterly,* 25(1), 43-70.

Chen, K. H. and Shimerda, T. A. (1981). An Empirical Analysis of Useful Financial Ratios, *Financial Management*, **10** (1), Spring, 51-60.

Dasgupta, S., Laplante, B. & Mamingi, N. (1998). Capital Market Responses to Environmental Performance in Developing Countries, Development Research Group, The World Bank, http://www.worldbank.org/nipr/work_paper/market/MARKETS-htmp2.htm April.

D'Amico, A. D. (2000). What Does a Computer Security Breach Really Cost? Secure Decisions, A Division of Applied Visions, Inc., September 7.

Dess, G. & Robinson, Jr., R. (1984). Measuring Organizational Performance in the Absence of Objective Measures: The Case of the Privately-held Firm and Conglomerate Business Unit, *Strategic Management Journal,* 5, 265-273.

Doherty, N. & Fulford, H. (2005). Do Information Security Policies Reduce the Incidence of Security Breaches: An Exploratory Analysis, *Information Resources Management Journal,* Oct – Dec, 18 (4), 21- 39.

Egan, M. & Mather, T. (2005). The Executive Guide to Information Security Threats, Challenges, and Solutions, Addison-Wesley, Indianapolis.

Erbschloe, M. (2005). Trojans, Worms, and Spyware, A Computer Security Professional's Guide to Malicious Code, Elsevier Butterworth Heinemann publishing, Bulington, MA.

Ezingeard, J.-N., McFadzean, E., & Birchall, D. (2005). A Model of Information Assurance Benefits, *Information Systems Management*, Spring, 20-29.

Featherman, M. S., Valacich, J. S. & Wells, J. D. (2006). Is That Authentic or Artifical? Understanding Consumer Perceptions of Risk in E-Service Encounters. *Information Systems Journal*, **16**, 107-134.

Garg, A., Curtis, J. & Halper, H. (2003a). The Financial Impact of IT Security Breaches: What Do Investors Think? *Information Systems Security*, March/April, 22-33.

Garg, A., Curtis, J. & Halper, H. (2003b). Quantifying the Financial Impact of IT Security Breaches, *Information Management & Computer Security*, **11** (2/3), 74-83.

Gordon, L., Loeb, M. P., Lucyshyn, W. & Richardson, R. (2004). 2004 CSI/FBI Computer Crime and Security Survey, Computer Security Institute.

Gordon, L., Loeb, M. P., Lucyshyn, W . & Ri chardson, R . (2005). 2005 CSI/FBI Com puter Crime and Security Survey, Computer Security Institute.

Grabosky, P. (2007). Electronic Crime. Pearson Prentice Hall, New Jersey.

Grover, V. & Saeed, K. A. (2004). Strategic Or ientation and Perform ance of Internet-Based Businesses, *Information Systems Journal*, **14**, 23 - 42.

Hitt, L., & Brynjolfsso n, E. (1996). Productivity, Business Profitability, and Consu mer Surplus: Three Different Measures of Information Technology Value. *MIS Quarterly,* **20** (2), 2, 121-142.

Hollander, Y. (2000). Prev ent W eb Site Defacem ent, *Internet Security Advisor*, November/December.

Hovav, A. & D'Arcy, J. (2004). Th e Impact of Virus a ttack announcements on the m arket value of firms. *Information Systems Security*, **13** (3) Jul/Aug, 32-40.

Hovav, A. & D'Arcy, J. (2003). The Im pact of Denial-of-Service Attack Announcem ents on the Market Value of Firms. *Risk Management and Insurance Review*, **6** (2), 97-121.

Hunton, J., Lippincott, B. & Reck, J. L. (2003) . Enterprise Resource Planning System s: Comparing Firm Perform ance of Adopters and Non-adopters. *International Journal of Accounting Information Systems,* **4**, 165-184.

Ko, M. and Dorantes C. (2006). The Im pact of Infor mation Secu rity Breaches on Financial Performance of the Breached Firm s: An Empirical In vestigation. *Journal of Information Technology Management*, 12, 13-22.

Nicolaou, A. L. (2004). Firm Performance Effects in Relation to the Im plementation and Use of Enterprise Resource Planning Systems. *Journal of Information Systems*, **18** (2), 79-105.

Pfleeger, C. (1997). The Fundamentals of Information Security, *IEEE Software*, **14** (1), 15 -17.

Ponemon Institu te (200 6). Ponem on Report Shows Sharp Rise in the Cost of Data Breaches, http://www.ponemon.org/press.html.

SecuritySearch.Com (2006). http://searchsecurity.techtarget.com/ accessed October, 16, 2007.

p://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214542,00.html

Snow, C. C. & Hrebiniak, L. G. (1980). Strate gy, Distinctive Com petence, and Organizational Performance, *Administrative Science Quarterly*, **25** (2), June, 317-336.

Solomon, M. G. & Chapple (2005). Inform ation Security Illum inated, Jones and Bartlett Publisher, Sudbury, Massachusetts.

Tsiakis, T. & Stephanides, G. (2005). The Economic Approach of Infor mation Security. *Computers & Security*, **24**, 105-108.

Warren, M. & Hutchinson, W . (2000). Cyber A ttacks against Supply Chain Managem ent Systems: A Short Note. *International Journal of Physical Distribution & Logistics Management,* **30** (7), 710-716.

Williams, R. & Joshi, A. (2004). Prot ection from Denial Serv ice Attack s, *http://telephonyonline.com/backoffice/infocus/telecom_protection_denial_service/*, Accessed October 16, 2007.

ENDNOTE:

1. This was obtained at http://www.cert.org.
2. There are 2 firms that had only one control firm each, thus, we used the industry SIC code to 1 digit to get more control firms for these 2 firms.

APPENDIX A: Samples of Publicly Announced Information Security Breaches

Source: The New York Times
Date: May 17, 2002
Title: 13000 Credit Reports Stolen by Hackers (A Single Breach Announcement)

BODY: Hackers posing as employees of the Ford Motor Credit Company have in recent months harvested a trove of 13,000 credit reports -- a virtual one-stop shop for fraud and identity theft -- with data on consumers in affluent neighborhoods across the country.
The company said in a letter to the victims that computer intruders used an authorization code from Ford Credit to get the credit reports from Experian, one of three major reporting agencies. "I've never seen anything of this size," a spokesman for Experian, Donald Girard, said. "Privacy is the hallmark of our business. We're extraordinarily concerned about the privacy issue here, and the trust factor." The inquiries gave the intruders access to each victim's personal and financial information, including address, Social Security number, bank and credit card accounts and ratings of creditworthiness, which can be used to identify the best targets.

Source: USA Today
Date: July 27, 2004
Title: MyDoom.M Virus Slams Search Sites (A Multiple Breach Announcement)

BODY: The latest version of the MyDoom e-mail virus, MyDoom.M, fooled tens of thousands of computer-savvy workers into triggering a disruption that knocked Internet search sites Google, Yahoo, Lycos and AltaVista off line for several hours Monday.